Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004

Boston Marriott Cambridge Hotel, Cambridge, MA, USA

August 10–13, 2004

Tuesday August 10, 2004

18:00 – 20:00 : Registration at Conference Hotel and Welcome Reception (wine and cheese)

Wednesday August 11, 2004

07:00 – : Registration continues

08:30 – 08:45 : Welcome to CHES 2004

08:45 – 10:00 : Session 1: Side Channels I

- Towards Efficient Second-Order Power Analysis
  Jason Waddle, David Wagner
- Correlation Power Analysis with a Leakage Model
  Eric Brier, Christophe Clavier, Francis Olivier
- Power Analysis of an FPGA
  François-Xavier Standaert, Siddika Berna Örs, Bart Preneel

10:00 – 10:30 : Coffee break

10:30 – 11:30 : Invited Talk I

- Physical Information Security
  Neil Gershenfeld (The Center for Bits and Atoms, MIT)

11:30 – 12:45 : Session 2: Modular Multiplication

- Long Modular Multiplication for Cryptographic Applications
  Laszlo Hars
- Leak Resistant Arithmetic
  Jean-Claude Bajard, Laurent Imbert, Pierre-Yvan Liardet, Yannick Teglia
- Efficient Linear Array for Multiplication in GF(2^m) Using a Normal Basis for Elliptic Curve Cryptography
  Soonhak Kwon, Kris Gaj, Chang Hoon Kim, Chun Pyo Hong

12:45 – 14:15 : Lunch

14:15 – 15:30 : Session 3: Low Resources I

- Low Power Elliptic Curve Cryptography Using Scaled Modular Arithmetic
  Erdinc Öztürk, Berk Sunar, Erkay Savaş
- A Low-cost ECC Coprocessor for Smartcards
  Harald Aigner, Holger Bock, Markus Hütter, Johannes Wolkerstorfer
- Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs
  Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, Sheueling Chang Shantz

15:30 – 16:00 : Coffee break

16:00 – 16:50 : Session 4: Implementation Aspects

- Instruction Set Extensions for Fast Arithmetic in Finite Fields GF(p) and GF(2^m)
  Johann Großschädl, Erkay Savaş
- Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementations
  Roberto Maria Avanzi

18:30 – 22:00 : Cruise Dinner (from Boston harbour)

Thursday August 12, 2004

08:30 – 09:20 : Session 5: Collision Attacks

- A Collision-Attack on AES
  Kai Schramm, Gregor Leander, Patrick Felke, Christof Paar
- Enhancing Collision Attacks
  Hervé Ledig, Frédéric Muller, Frédéric Valette

09:20 – 10:10 : Session 6: Side Channels II

- Simple Power Analysis of Unified Code for ECC Double and Add
  Colin D. Walter
- DPA on n-bit sized Boolean and Arithmetic Operations and its Application to IDEA, RC6 and the HMAC-Construction
  Kerstin Lemke, Kai Schramm, Christof Paar

10:10 – 10:40 : Coffee break

10:40 – 11:30 : Session 6 (cont'd): Side Channels II

- Side-Channel Attacks in ECC: A General Technique for Varying the Parametrization of the Elliptic Curve
  Loren D. Olson
- Switching Blindings
  Olaf Neiße, Jürgen Pulkus

11:30 – 12:20 : Session 7: Fault Attacks

- Fault Analysis of Stream Ciphers
  Jonathan J. Hoch, Adi Shamir
- A Differential Fault Attack Against Early Rounds of (Triple-)DES
  Ludger Hemme

12:20 – 14:00 : Lunch

14:00 - 14:50 : Session 8: Hardware Implementation I

- An Offset-compensated Oscillator-based Random Bit Source for Security Applications
  Holger Bock, Marco Bucci, Raimondo Luzzi
- Improving the Security of Dual-Rail Circuits
  Danil Sokolov, Julian Murphy, Alex Bystrov, Alex Yakovlev

14:50 – 15:50 : Invited Talk II

- Quantum Cryptography
  Isaac Chuang (Medialab, MIT)

15:50 – 16:20 : Coffee break

16:20 – 18:00 : Session 9: Side Channels III

- A New Attack with Side Channel Leakage during Exponent Recoding Computations
  Yasuyuki Sakai, Kouichi Sakurai
- Defeating Countermeasures Based on Randomized BSD Representations
  Pierre-Alain Fouque, Frédéric Muller, Guillaume Poupard, Frédéric Valette
- Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems
  Pradeep Kumar Mishra
- Efficient Countermeasures against RPA, DPA, and SPA
  Hideyo Mamiya, Atsuko Miyaji, Hiroaki Morimoto

19:00 – 20:30 : Dinner (hotel)

20:30 – : Rump Session (Chair: Christof Paar)

Friday August 13, 2004

09:00 – 10:00 : Invited Talk III

- From Proof to Practice: Real-World Cryptography
  Paul Kocher (Cryptography Research)

10:00 – 10:30 : Coffee break

10:30 – 11:20 : Session 10: Low Resources II

- Strong Authentication for RFID Systems using the AES Algorithm
  Martin Feldhofer, Sandra Dominikus, Johannes Wolkerstorfer
- TTS: High-Speed Signatures on a Low-Cost Smart Card
  Bo-Yin Yang, Jiun-Ming Chen, Yen-Hung Chen

11:20 – 12:10 : Session 11: Hardware Implementation II

- XTR Implementation in Reconfigurable Hardware
  Eric Peeters, Michaël Nève, Mathieu Ciet
- Concurrent Error Detection Schemes for Involution Ciphers
  Nikhil Joshi, Kaijie Wu, Ramesh Karri

12:10 – 13:40 : Lunch

13:40 – 14:55 : Session 12: Authentication and Signatures

- Public Key Authentification with one (on-line) Single Addition
  Marc Girault, David Lefranc
- Attacking DSA under a Repeated Bits Assumption
  Peter J. Leadbitter, Dan Page, Nigel P. Smart
- How to Disembed a Program?
  Benoît Chevallier-Mames, David Naccache, Pascal Paillier, David Pointcheval

14:55 – 15:00 : Best Paper Award(s) and Concluding Remarks